UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

ELAINE D. MALINOWSKI, individually, and on behalf of all others similarly situated, Plaintiffs, vs. INTERNATIONAL BUSINESS MACHINES CORPORATION and JOHNSON & JOHNSON HEALTH CARE SYSTEMS, INC., Defendant.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Representative Plaintiff alleges as follows:

INTRODUCTION

1. Representative Plaintiff Elaine Malinowski ("Representative Plaintiff") bring this Class Action Complaint against Defendants International Business Machines Corporation ("IBM") and Johnson & Johnson Health Care Systems, Inc. ("Johnson") (collectively, "Defendants") for their failure to properly secure and safeguard Representative Plaintiff's and Class Members' protected health information and personally identifiable information stored within Defendants' information network, including, without limitation, full names, contact information, and information about medications and associated conditions (these types of information, *inter*

alia, being thereafter referred to, collectively, as "protected health information" or "PHI"[1] and "personally identifiable information" or "PII").[2]

2. With this action, Representative Plaintiff seek to hold Defendants responsible for the harms it caused and will continue to cause Representative Plaintiff and, at least, thousands of other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendants on August 2, 2023, in which cybercriminals infiltrated Defendants' inadequately protected network servers and accessed highly sensitive PHI/PII that was being kept unprotected ("Data Breach").

3. Representative Plaintiff further seeks to hold Defendants responsible for not ensuring that PHI/PII was maintained in a manner consistent with industry, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule (45 CFR, Part 160 and Parts A and E of Part 164), the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164), and other relevant standards.

4. While Defendants claims to have discovered the breach as early as August 2, 2023, Defendants did not inform victims of the Data Breach until September 15, 2023. Indeed, Representative Plaintiff and Class Members were wholly unaware of the Data Breach until they received letters from Defendants informing them of it.

---

[1] Protected health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

5. Defendants acquired, collected, and stored Representative Plaintiff's and Class Members' PHI/PII. Therefore, at all relevant times, Defendants knew or should have known that Representative Plaintiff and Class Members would use Defendants' services to store and/or share sensitive data, including highly confidential PHI/PII.

6. HIPAA establishes national minimum standards for protecting individuals' medical records and other protected health information. HIPAA, generally, applies to health plans/insurers, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically and sets minimum standards for Defendants' maintenance of Representative Plaintiff's and Class Members' PHI/PII. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendants to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization. HIPAA also establishes a series of rights over Representative Plaintiff's and Class Members' PHI/PII, including rights to examine and obtain copies of their health records and to request corrections thereto.

7. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

8. By obtaining, collecting, using, and deriving a benefit from Representative Plaintiff's and Class Members' PHI/PII, Defendants assumed legal and equitable duties to those individuals. These duties arise from HIPAA, other state and federal statutes and regulations, and common law principles. Representative Plaintiff do not bring claims in this action for direct

violations of HIPAA but charge Defendants with various legal violations merely predicated upon the duties set forth in HIPAA.

9. Defendants disregarded the rights of Representative Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiff's and Class Members' PHI/PII was safeguarded, failing to take available steps to prevent unauthorized disclosure of data and failing to follow applicable, required and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, Representative Plaintiff's and Class Members' PHI/PII was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Representative Plaintiff and Class Members in the future. Representative Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe and are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

10. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant.

11. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

12. Defendants are33 headquartered and/or routinely conducts business in the State where this District is located, has sufficient minimum contacts in this State, has intentionally

availed itself of this jurisdiction by marketing and/or selling products and/or services and/or by accepting and processing payments for those products and/or services within this State.

13. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Representative Plaintiff's claims took place within this District and Defendants is headquartered and/or does business in this Judicial District.

REPRESENTATIVE PLAINTIFF'S COMMON EXPERIENCES

14. Defendants received highly sensitive PHI/PII from Representative Plaintiff in connection with the services and/or employment Representative Plaintiff received or requested. As a result, Representative Plaintiff's information was among the data an unauthorized third party accessed in the Data Breach.

15. Representative Plaintiff was and ais very careful about sharing her PHI/PII. Representative Plaintiff has never knowingly transmitted unencrypted sensitive PHI/PII over the internet or any other unsecured source.

16. Representative Plaintiff stored any documents containing their PHI/PII in a safe and secure location or destroyed the documents. Moreover, Representative Plaintiff diligently chose unique usernames and passwords for her various online accounts.

17. Representative Plaintiff took reasonable steps to maintain the confidentiality of her PHI/PII and relied on Defendants to keep her PHI/PII confidential and securely maintained, and to make only authorized disclosures of this information.

18. The Notice from Defendants (the website version of this Notice, which is substantially similar in content to the Notices received by Representative Plaintiff and the Class, is attached as **Exhibit A**) notified Representative Plaintiff that Defendants' network had been accessed and that Plaintiff's PHI/PII may have been involved in the Data Breach.

19. Furthermore, Defendants' Notice directed Representative Plaintiff to be vigilant and to take certain steps to protect their PHI/PII and otherwise mitigate their damages.

20. As a result of the Data Breach, Plaintiff heeded Defendants' warnings and spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice and self-monitoring their accounts and credit reports to ensure no fraudulent activity had occurred. This time has been lost forever and cannot be recaptured.

21. Representative Plaintiff suffered actual injury in the form of damages to and diminution in the value of Representative Plaintiff's PHI/PII—a form of intangible property that Representative Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach.

22. Representative Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and have anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling Representative Plaintiff's PHI/PII.

23. Representative Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PHI/PII, in combination with their names, being placed in the hands of unauthorized third parties/criminals.

24. Representative Plaintiff have a continuing interest in ensuring that Representative Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

//

//

//

Plaintiff Elaine Malinowski's Experiences

25. On or about September 15, 2023, Representative Plaintiff was notified via letter from Defendants that her PHI and/or PII had been accessed because of the Data Breach.

26. Representative Plaintiff is an adult individual and, at all times relevant herein, a resident and citizen of the State of Florida. Representative Plaintiff is a victim of the Data Breach. Defendants were admittedly in possession of Representative Plaintiff's PHI/PII.

27. As a result, Representative Plaintiff's information was among the data an unauthorized third party accessed in the Data Breach.

28. Representative Plaintiff regularly monitors her credit and identity for fraudulent activity since the Breach.

29. Representative Plaintiff is made uncomfortable because her personal information and all of her health information is out there.

DEFENDANT

30. Defendants IBM is a New York corporation with a principal place of business located at One Orchard Road Armonk, NY 10504.

31. Defendants IBM provides "infrastructure, software, and consulting services for clients as they pursue the digital transformation of the world's mission-critical businesses."[3]

32. Defendants Johnson & Johnson Health Care Systems, Inc. is a New Jersey corporation with a principal place of business located at 425 Hoes Lane Piscataway, NJ 08854.

33. Defendants Johnson & Johnson Health Care Systems Inc., which owns Jansenn Carepath, provides contracting, supply chain, and business support services.[4]

[3] IBM, *About IBM:* https://www.ibm.com/about?lnk=fab (Last accessed September 22, 2023)
[4] Bloomberg Company Profile: https://www.bloomberg.com/profile/company/0008005D:US#xj4y7vzkg (Last accessed September 22, 2023)

34. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiffs. Representative Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

35. Representative Plaintiff bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure ("F.R.C.P.") on behalf of Representative Plaintiff and the following classes/subclass(es) (collectively, the "Class(es)"):

> **Nationwide Class:**
> "All individuals within the United States of America whose PHI/PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendants on September 15, 2023."

36. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers, and directors and any entity in which Defendants has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsel, and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

37. In the alternative, Representative Plaintiff requests additional subclasses as necessary based on the types of PHI/PII that were compromised.

38. Representative Plaintiff reserves the right to amend the above Class definitions or to propose other subclasses in subsequent pleadings and motions for class certification.

39. This action has been brought and may properly be maintained as a class action under F.R.C.P. Rule 23 because there is a well-defined community of interest in the litigation and membership of the proposed Classes is readily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiff is informed and believe and, on that basis, allege that the total number of Class Members is in the thousands of individuals. Membership in the Classes will be determined by analysis of Defendants' records.

b. Commonality: Representative Plaintiff and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendants had a legal duty to Representative Plaintiff and the Classes to exercise due care in collecting, storing, using and/or safeguarding their PHI/PII;

2) Whether Defendants knew or should have known of the susceptibility of their data security systems to a data breach;

3) Whether Defendants' security procedures and practices to protect their systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendants' failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendants failed to comply with their own policies and applicable laws, regulations and industry standards relating to data security;

6) Whether Defendants adequately, promptly and accurately informed Representative Plaintiff and Class Members that their PHI/PII had been compromised;

7) How and when Defendants actually learned of the Data Breach;

8) Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the loss of the PHI/PII of Representative Plaintiff and Class Members;

9) Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendants engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiff's and Class Members' PHI/PII;

11) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendants' wrongful conduct;

12) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

c. Typicality: Representative Plaintiff's claims are typical of the claims of the Plaintiff Classes. Representative Plaintiff and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendants' common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiff in this class action is an adequate representative of each of the Plaintiff Classes in that Representative Plaintiff have the same interest in the litigation of this case as the Class Members, are committed to the vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in their entirety. Representative Plaintiff anticipates no management difficulties in this litigation.

e. Superiority of Class Action: The damages suffered by individual Class Members are significant but may be small relative to each member's enormous expense of individual litigation. This makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately. Individualized litigation increases the delay and expense to all parties and to the court system, presented by the case's complex legal and factual issues. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale and comprehensive supervision by a single court.

40. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, so it is impracticable to bring all Class Members before the Court.

41. This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate concerning the Classes in their entireties. Defendants' policies and practices challenged herein apply to and affect Class Members uniformly. Representative Plaintiff's challenge of these policies and procedures hinges on Defendants' conduct concerning the Classes in their entirety, not on facts or law applicable only to Representative Plaintiff.

42. Unless a Class-wide injunction is issued, Defendants may continue failing to secure Class Members' PHI/PII properly, and Defendants may continue to act unlawfully, as set forth in this Complaint.

43. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under F.R.C.P. Rule 23(b)(2).

COMMON FACTUAL ALLEGATIONS

The Data Breach

44. During the Data Breach, one or more unauthorized third parties accessed Class Members' sensitive data including, but not limited full names, contact information, and information about medications and associated conditions. Representative Plaintiff was among the individuals whose data was accessed in the Data Breach.

45. According to Defendants IBM the Data Breach occurred when an unauthorized actor accessed the IBM-managed "application and third-party database that supports Janssen CarePath." **Exhibit A.**

46. Representative Plaintiff was provided the information detailed above upon Representative Plaintiff's receipt of a Defendants' Notice. Representative Plaintiff was not aware of the Data Breach until receiving this letter.

47. Since Notice was not sent until September 2023, an unauthorized actor had access to the PII for over a month without the account being secured or the Breach being discovered.

Defendants' Failed Response to the Data Breach

48. Not until roughly two months after it claims to have discovered the Data Breach did Defendants begin sending the Notice to persons whose PHI/PII Defendants confirmed was potentially compromised because of the Data Breach. The Notice provided basic details of the Data Breach and Defendants' recommended next steps.

49. The Notice included, *inter alia*, the claims that Defendants had learned of the Data Breach on August 2, 2023, and had taken steps to respond. But the Notice lacked sufficient information on how the breach occurred, what safeguards have been taken since then to safeguard further attacks, and/or where the information hacked exists today.

50. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiff's and Class Members' PHI/PII with the intent of misusing the PHI/PII, including marketing and selling Representative Plaintiff's and Class Members' PHI/PII.

51. Defendants had and continue to have obligations created by HIPAA, applicable federal and state law as set forth herein, reasonable industry standards, common law, and their own

assurances and representations to keep Representative Plaintiff's and Class Members' PHI/PII confidential and to protect such PHI/PII from unauthorized access.

52. Defendants collected and stored Representative Plaintiff's and Class Members' PHI/PII with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

53. Despite this, even today, Representative Plaintiff and Class Members remain in the dark regarding what data was stolen, the particular malware used, and what steps are being taken to secure their PHI/PII in the future. Thus, Representative Plaintiff and Class Members are left to speculate as to where their PHI/PII ended up, who has used it, and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how Defendants intends to enhance their information security systems and monitoring capabilities to prevent further breaches.

54. Representative Plaintiff's and Class Members' PHI/PII may end up for sale on the dark web or fall into the hands of companies that will use the detailed PHI/PII for targeted marketing without Representative Plaintiff's and/or Class Members' approval. Either way, unauthorized individuals can now easily access Representative Plaintiff's and Class Members' PHI/PII.

Defendants Collected/Stored Representative Plaintiff's and Class Members' PHI/PII

55. Defendants acquired, collected, stored, and assured reasonable security over Representative Plaintiff's and Class Members' PHI/PII.

56. As a condition of their relationships with Representative Plaintiff and Class Members, Defendants required that Representative Plaintiff and Class Members entrust

Defendants with highly sensitive and confidential PHI/PII. Defendants, in turn, stored that information on Defendants' system that was ultimately affected by the Data Breach.

57. By obtaining, collecting, and storing Representative Plaintiff's and Class Members' PHI/PII, Defendants assumed legal and equitable duties over the PHI/PII and knew or should have known that it was thereafter responsible for protecting Representative Plaintiff's and Class Members' PHI/PII from unauthorized disclosure.

58. Representative Plaintiff and Class Members have taken reasonable steps to maintain their PHI/PII's confidentiality. Representative Plaintiff and Class Members relied on Defendants to keep their PHI/PII confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

59. Defendants could have prevented the Data Breach, which began as early as August 2023, by properly securing and encrypting and/or more securely encrypting their servers, generally, as well as Representative Plaintiff's and Class Members' PHI/PII.

60. Defendants' negligence in safeguarding Representative Plaintiff's and Class Members' PHI/PII is exacerbated by repeated warnings and alerts directed at protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

61. The healthcare industry has experienced many high-profile cyberattacks in the last several years preceding this Complaint's filing. Cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year,

showing a 25% increase.[5] According to the HIPAA Journal, the largest healthcare data breaches were reported in April 2021.[6]

62. For example, Universal Health Services experienced a cyberattack on September 29, 2020, similar to the attack on Defendant. As a result of this attack, Universal Health Services suffered a four-week outage of its systems which caused as much as $67 million in recovery costs and lost revenue.[7] Similarly, in 2021, Scripps Health suffered a cyberattack, which effectively shut down critical healthcare services for a month and left numerous patients unable to speak to their physicians or access vital medical and prescription records.[8] University of San Diego Health suffered a similar attack a few months later.[9]

63. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[10]

64. The HIPAA Journal article explains that patient records, like those stolen from Defendant, are "often processed and packaged with other illegally obtained data to create full record sets (full) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals, which "allows an identity kit to be

---

[5] https://www.hipaajournal.com/2020-healthcare-data-breach-report/ (last accessed July 24, 2023).

[6] https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/ (last accessed July 24, 2023).

[7] https://www.prnewswire.com/news-releases/universal-health-services-inc-reports-2020-fourth-quarter-and-full-year-financial-results-and-2021-full-year-earnings-guidance-301236075.html/ (last accessed July 24, 2023).

[8] https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/ (last accessed July 24, 2023).

[9] https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-employee-email-accounts-impacted/2670302/ (last accessed July 24, 2023).

[10] *Editorial: Why Do Criminals Target Medical Records,* HIPAA J. (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/

created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[11]

65. Data breaches such as the one experienced by Defendants have become so notorious that the Federal Bureau of Investigation ("FBI") and the U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully ward off a potential attack.

66. Due to the high-profile nature of these breaches and other breaches of its kind, Defendants was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack.

67. And yet, despite the prevalence of public announcements of data breaches and data security compromises, Defendants failed to take appropriate steps to protect Representative Plaintiff's and Class Members' PHI/PII from being compromised.

Defendants Had a Duty to Protect the Stolen Information

68. In failing to adequately secure Representative Plaintiff's and Class Members' sensitive data, Defendants breached duties they owed Representative Plaintiff and Class Members under statutory and common law. Under HIPAA, health insurance providers and business associates have an affirmative duty to keep patients' protected health information private. As a covered entity, Defendants have a statutory duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiff's and Class Members' data. Moreover, Representative Plaintiff and Class Members surrendered their highly sensitive personal data to Defendants under

[11] *Id.*

the implied condition that Defendants would keep it private and secure. Accordingly, Defendants also had an implied duty to safeguard their data, independent of any statute.

69. Because Defendants are covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

70. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for protecting health information.

71. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

72. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

73. "Electronic protected health information" is "individually identifiable health information […] that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

74. HIPAA's Security Rule requires Defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

75. HIPAA also requires Defendants to "review and modify the security measures implemented […] as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

76. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

77. Defendants were also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

78. According to the FTC, the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendants, should employ to protect against the unlawful exposure of PHI/PII.

79. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that companies should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of PHI/PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

80. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

81. The FTC recommends that companies not maintain information longer than is necessary for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network and verify that third-party service providers have implemented reasonable security measures.

82. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

83. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PHI/PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

84. In addition to their obligations under federal and state laws, Defendants owed a duty to Representative Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII in Defendants' possession

from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Representative Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected Representative Plaintiff's and Class Members' PHI/PII.

85. Defendants owed a duty to Representative Plaintiff and Class Members to design, maintain, and test their computer systems, servers, and networks to ensure that all PHI/PII in their possession was adequately secured and protected.

86. Defendants owed a duty to Representative Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect all PHI/PII in their possession, including not sharing information with other entities who maintain sub-standard data security systems.

87. Defendants owed a duty to Representative Plaintiff and Class Members to implement processes that would immediately detect a breach of their data security systems in a timely manner.

88. Defendants owed a duty to Representative Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

89. Defendants owed a duty to Representative Plaintiff and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PHI/PII from theft, because such an inadequacy would be a material fact in the decision to entrust this PHI/PII to Defendants.

90. Defendants owed a duty of care to Representative Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

91. Defendants owed a duty to Representative Plaintiff and Class Members to encrypt and/or more reliably encrypt Representative Plaintiff's and Class Members' PHI/PII and monitor user behavior and activity to identify possible threats.

The Sensitive Information Stolen in the Data Breach is Highly Valuable

92. It is well known that PHI/PII, including Social Security numbers and health records in particular, are a valuable commodity and a frequent, intentional target of cybercriminals. Companies that collect such information, including Defendants, are well aware of the risk of being targeted by cybercriminals.

93. Individuals place a high value not only on their PHI/PII but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight the impact of identity theft.

94. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a lot of sensitive information (e.g., patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the healthcare industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

95. The high value of PHI/PII to criminals is evidenced by the prices they will pay for it through the dark web. For example, personal information can be sold at a price ranging from

$40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[13] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[14]

96. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[15] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[16] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[17]

97. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiff and Class Members. For example, it is believed that certain PHI/PII compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

98. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other

---

[12] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 24, 2023).

[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July 24, 2023).

[14] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 24, 2023).

[15] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed July 24, 2023).

[16] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed July 24, 2023).

[17] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/ (last accessed July 24, 2023).

information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

99. Identity thieves can use PHI/PII, such as that of Representative Plaintiff and Class Members which Defendants failed to keep secure, to perpetrate various crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

100. The ramifications of Defendants' failure to secure Representative Plaintiff's and Class Members' PHI/PII are long-lasting and severe. Once PHI/PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PHI/PII of Representative Plaintiff and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PHI/PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

101. Individuals, like Representative Plaintiff and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and are likened to accessing DNA for hacker's purposes.

102. Data breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Representative Plaintiff and Class Members cannot obtain new numbers unless they become victims of Social Security misuse.

103. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[18]

104. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI/PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

105. The harm to Representative Plaintiff and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," more than identity thefts involving banking and finance, the government, and the military or education.[20]

106. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy

---

[18] *Identity Theft and Your Social Security Number*, SSA, No. 05-10064 (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 18, 2023).
[19] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed July 24, 2023).
[20] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed July 24, 2023).

Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[21]

107. When cybercriminals access financial information, health insurance information, and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendants may have exposed Representative Plaintiff and Class Members.

108. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[22] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[23]

109. And data breaches are preventable.[24] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[25] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised…."[26]

---

[21] *Id.*
[22] See Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed July 24, 2023).
[23] Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed July 24, 2023).
[24] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[25] *Id.* at 17.
[26] *Id.* at 28.

110. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. Appropriate information security controls, including encryption, must be implemented and enforced rigorously and disciplined so that a *data breach never occurs*.[27]

111. Here, Defendants knew of the importance of safeguarding PHI/PII and of the foreseeable consequences that would occur if Representative Plaintiff's and Class Members' PHI/PII was stolen, including the significant costs that would be placed on Representative Plaintiff and Class Members because of a breach of this magnitude. As detailed above, Defendants knew or should have known that the development and use of such protocols was necessary to fulfill their statutory and common law duties to Representative Plaintiff and Class Members. Therefore, their failure to do so is intentional, willful, reckless, and/or grossly negligent.

112. Furthermore, Defendants have offered only a limited one-year subscription for identity theft monitoring and identity theft protection through Equifax. their limitation is inadequate when the victims will likely face many years of identity theft.

113. Moreover, Defendants' credit monitoring offer and advice to Representative Plaintiff and Class Members squarely place the burden on Representative Plaintiff and Class Members, rather than on Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendants expects Representative Plaintiff and Class Members to protect themselves from their tortious acts resulting from the Data Breach. Rather than automatically enrolling Representative Plaintiff and Class Members in credit monitoring services upon discovery of the Data Breach, Defendants merely sent instructions to Representative Plaintiff and Class Members about actions they could affirmatively take to protect themselves.

[27] *Id.*

114. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Representative Plaintiff's and Class Members' PHI/PII.

115. Defendants disregarded the rights of Representative Plaintiff and Class Members by, *inter alia*: (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions, (ii) failing to disclose that it did not have adequate security protocols and training practices in place to safeguard Representative Plaintiff's and Class Members' PHI/PII, (iii) failing to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time, and (v) failing to provide Representative Plaintiff and Class Members prompt and accurate notice of the Data Breach.

CAUSES OF ACTION

COUNT ONE
Negligence
(On behalf of the Nationwide Class)

116. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

117. At all times herein relevant, Defendants owed Representative Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII and to use commercially reasonable methods to do so. Defendants took on this obligation upon accepting and storing Representative Plaintiff's and Class Members' PHI/PII on their computer systems and networks.

118. Among these duties, Defendants was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in their possession;

b. to protect Representative Plaintiff's and Class Members' PHI/PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to act on warnings about data breaches timely; and

d. to promptly notify Representative Plaintiff and Class Members of any data breach, security incident or intrusion that affected or may have affected their PHI/PII.

119. Defendants knew or should have known that the PHI/PII was private and confidential and should be protected as private and confidential and, thus, Defendants owed a duty of care to not subject Representative Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

120. Defendants knew or should have known of the risks inherent in collecting and storing PHI/PII, the vulnerabilities of their data security systems and the importance of adequate security. Defendants knew or should have known about numerous well-publicized data breaches.

121. Defendants knew or should have known that their data systems and networks did not adequately safeguard Representative Plaintiff's and Class Members' PHI/PII.

122. Only Defendants was in the position to ensure that their systems and protocols were sufficient to protect the PHI/PII that Representative Plaintiff and Class Members had entrusted to it.

123. Defendants breached their duties to Representative Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PHI/PII.

124. Because Defendants knew that a breach of their systems could damage numerous individuals, including Representative Plaintiff and Class Members, Defendants had a duty to adequately protect their data systems and the PHI/PII stored thereon.

125. Representative Plaintiff's and Class Members' willingness to entrust Defendants with their PHI/PII was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants could protect their systems and the PHI/PII it stored on them from attack. Thus, Defendants had a special relationship with Representative Plaintiff and Class Members.

126. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Representative Plaintiff's and Class Members' PHI/PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant, Representative Plaintiffs, and/or the remaining Class Members.

127. Defendants breached their general duty of care to Representative Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable and/or adequate computer systems and data security practices to safeguard Representative Plaintiff's and Class Members' PHI/PII;

b. by failing to timely and accurately disclose that Representative Plaintiff's and Class Members' PHI/PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard PHI/PII by knowingly disregarding standard information security principles, despite obvious risks and by allowing unmonitored and unrestricted access to unsecured PHI/PII;

d. by failing to provide adequate supervision and oversight of the PHI/PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Representative Plaintiff's and Class Members' PHI/PII, misuse the PHI/PII and intentionally disclose it to others without consent;

e. by failing to adequately train their employees not to store ger than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiff's and Class Members' PHI/PII;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt Representative Plaintiff's and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

128. Defendants' willful failure to abide by these duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

129. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Representative Plaintiff and Class Members have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

130. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PHI/PII to Representative Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PHI/PII.

131. Defendants breached their duty to notify Representative Plaintiff and Class Members of the unauthorized access by waiting roughly two months after learning of the Data Breach to notify Representative Plaintiff and Class Members and then by failing and continuing to fail to provide Representative Plaintiff and Class Members sufficient information regarding the breach. To date, Defendants has not provided sufficient information to Representative Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach their disclosure obligations to Representative Plaintiff and Class Members.

132. Further, explicitly failing to provide timely and clear notification of the Data Breach to Representative Plaintiff and Class Members, Defendants prevented Representative Plaintiff and Class Members from taking meaningful, proactive steps to secure their PHI/PII and access their medical records and histories.

133. There is a close causal connection between Defendants' failure to implement security measures to protect Representative Plaintiff's and Class Members' PHI/PII and the harm (or risk of imminent harm suffered) by Representative Plaintiff and Class Members.

Representative Plaintiff's and Class Members' PHI/PII was accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PHI/PII by adopting, implementing and maintaining appropriate security measures.

134. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

135. The damages Representative Plaintiff and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

136. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair […] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI/PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

137. Defendants violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PHI/PII and by not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PHI/PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiff and Class Members.

138. Defendants' violation of 15 U.S.C. § 45 constitutes negligence *per se*. Defendants also violated the HIPAA Privacy and Security rules, which constitutes negligence *per se*.

139. As a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their

PHI/PII is used, (iii) the compromise, publication, and/or theft of their PHI/PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft, (vi) lost continuity in relation to their healthcare, (vii) the continued risk to their PHI/PII, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Representative Plaintiff's and Class Members' PHI/PII in their continued possession, and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiff and Class Members.

140. As a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

141. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to suffer the continued risks of exposure of their PHI/PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PHI/PII in their continued possession.

//

COUNT TWO
Negligence *Per Se*
(On behalf of the Nationwide Class)

142. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

143. HIPAA requires that covered entities and business associates "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information" and "must reasonably safeguard protected health information from any intentional or unintentional use or disclosure…." 45 CFR § 164.530I.

144. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 requires HIPAA covered entities and their business associates to provide notification to the United States Department of Health and Human Services, prominent media outlets following a data breach or any breach of unsecured protected health information without unreasonable delay and in no event later than 60 days after discovery of a data breach.

145. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 prohibits companies such as Defendants from "using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce," including failing to use reasonable measures to protect PHI/PII. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

146. In addition to the FTC rules and regulations and state law, other states and jurisdictions where victims of the Data Breach are located require that Defendants protect PHI/PII from unauthorized access and disclosure and timely notify the victim of a data breach.

147. Defendants violated HIPAA and FTC rules and regulations obligating companies to use reasonable measures to protect PHI/PII by failing to comply with applicable industry standards and by unduly delaying reasonable notice of the actual breach. Defendants' conduct was particularly unreasonable given the nature and amount of PHI/PII it obtained and stored and the foreseeable consequences of a Data Breach and the exposure of Representative Plaintiff's and Class members' highly sensitive PHI/PII.

148. Each of Defendants' statutory violations of HIPAA, Section 5 of the FTC Act and other applicable statutes, rules and regulations, constitute negligence *per se*.

149. Representative Plaintiff and Class Members are within the category of persons HIPAA and the FTC Act were intended to protect.

150. The harm that occurred because of the Data Breach described herein is the type of harm HIPAA and the FTC Act were intended to guard against.

151. As a direct and proximate result of Defendants' negligence *per se*, Representative Plaintiff and Class Members have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PHI/PII in Defendants' possession and are entitled to damages in an amount to be proven at trial.

COUNT THREE
Breach of Confidence
(On behalf of the Nationwide Class)

152. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

153. During Representative Plaintiff's and Class Members' interactions with Defendant, Defendants was fully aware of the confidential nature of the PHI/PII that Representative Plaintiff and Class Members provided to it.

154. As alleged herein and above, Defendants' relationship with Representative Plaintiff and Class Members was governed by promises and expectations that Representative Plaintiff and Class Members' PHI/PII would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

155. Representative Plaintiff and Class Members provided their respective PHI/PII to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PHI/PII to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

156. Representative Plaintiff and Class Members also provided their PHI/PII to Defendants with the explicit and implicit understanding that Defendants would take precautions to protect their PHI/PII from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting their networks and data systems.

157. Defendants voluntarily received, in confidence, Representative Plaintiff's and Class Members' PHI/PII with the understanding that the PHI/PII would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

158. Due to Defendants' failure to prevent, detect and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices to secure Representative Plaintiff's and Class Members' PHI/PII, Representative Plaintiff's and Class Members' PHI/PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by,

released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Representative Plaintiff's and Class Members' confidence and without their express permission.

159. As a direct and proximate cause of Defendants' actions and/or omissions, Representative Plaintiff and Class Members have suffered damages, as alleged herein.

160. But for Defendants' failure to maintain and protect Representative Plaintiff's and Class Members' PHI/PII in violation of the parties' understanding of confidence, their PHI/PII would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. The Data Breach was the direct and legal cause of the misuse of Representative Plaintiff's and Class Members' PHI/PII and the resulting damages.

161. The injury and harm Representative Plaintiff and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendants' unauthorized misuse of Representative Plaintiff's and Class Members' PHI/PII. Defendants knew their data systems and protocols for accepting and securing Representative Plaintiff's and Class Members' PHI/PII had security and other vulnerabilities that placed Representative Plaintiff's and Class Members' PHI/PII in jeopardy.

162. As a direct and proximate result of Defendants' breaches of confidence, Representative Plaintiff and Class Members have suffered and will continue to suffer injury, as alleged herein, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PHI/PII, (iii) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their PHI/PII, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but

not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, (v) the continued risk to their PHI/PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Class Members' PHI/PII in their continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Representative Plaintiff and Class Members, (vii) the diminished value of Representative Plaintiff's and Class Members' PHI/PII, and (viii) the diminished value of Defendants' services for which Representative Plaintiff and Class Members paid and received.

COUNT FOUR
Breach of Implied Contract
(On behalf of the Nationwide Class)

163. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

164. Through their course of conduct, Defendant, Representative Plaintiff and Class Members entered into implied contracts for Defendants to implement data security adequate to safeguard and protect the privacy of Representative Plaintiff's and Class Members' PHI/PII.

165. Defendants required Representative Plaintiff and Class Members to provide and entrust their PHI/PII as a condition of obtaining Defendants' services.

166. Defendants solicited and invited Representative Plaintiff and Class Members to provide their PHI/PII as part of Defendants' regular business practices. Representative Plaintiff and Class Members accepted Defendants' offers and provided their PHI/PII to Defendant.

167. As a condition of being Defendants' direct patients, Representative Plaintiff and Class Members provided and entrusted their PHI/PII to Defendant. In so doing, Representative Plaintiff and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such non-public information, to keep such information secure and

confidential and to timely and accurately notify Representative Plaintiff and Class Members if their data had been breached and compromised or stolen.

168. A meeting of the minds occurred when Representative Plaintiff and Class Members agreed to, and did, provide their PHI/PII to Defendant, in exchange for, amongst other things, the protection of their PHI/PII.

169. Representative Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

170. Defendants breached the implied contracts it made with Representative Plaintiff and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate notice to them that their PHI/PII was compromised because of the Data Breach.

As a direct and proximate result of Defendants' above-described breach of implied contract, Representative Plaintiff and Class Members have suffered and will continue to suffer: (i) ongoing, imminent and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (vi) other economic and non-economic harm.

COUNT FIVE
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Nationwide Class)

171. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

172. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

173. Representative Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

174. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI/PII, failing to timely and accurately disclose the Data Breach to Representative Plaintiff and Class Members, and continued acceptance of PHI/PII and storage of other personal information after Defendants knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

175. Defendants acted in bad faith and/or with malicious motive in denying Representative Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT SIX
Breach of Fiduciary Duty
(On behalf of the Nationwide Class)

176. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

177. In light of the special relationship between Defendants and Representative Plaintiff and Class Members, whereby Defendants became the guardian of Representative Plaintiff's and Class Members' PHI/PII, Defendants became a fiduciary by their undertaking and guardianship of the PHI/PII to act primarily for Representative Plaintiff and Class Members, (i) for the safeguarding of Representative Plaintiff's and Class Members' PHI/PII, (ii) to timely notify Representative Plaintiff and Class Members of a data breach and disclosure, and (iii) to maintain complete and accurate records of what information (and where) Defendants did has and continues to store.

178. Defendants has a fiduciary duty to act for the benefit of Representative Plaintiff and Class Members upon matters within the scope of their relationship with Class Members—in particular, to keep their PHI/PII secure.

179. Defendants breached their fiduciary duties to Representative Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

180. Defendants breached their fiduciary duties to Representative Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Representative Plaintiff's and Class Members' PHI/PII.

181. Defendants breached their fiduciary duties to Representative Plaintiff and Class Members by failing to timely notify and/or warn Representative Plaintiff and Class Members of the Data Breach.

182. Defendants breached their fiduciary duties to Representative Plaintiff and Class Members by otherwise failing to safeguard Representative Plaintiff's and Class Members' PHI/PII.

183. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Representative Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PHI/PII, (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PHI/PII, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, contest, and recover from identity theft, (v) the continued risk to their

PHI/PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PHI/PII in their continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Representative Plaintiff and Class Members, and (vii) the diminished value of Defendants' services they received.

184. As a direct and proximate result of Defendants' breach of their fiduciary duties, Representative Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT SEVEN
Unjust Enrichment
(On behalf of the Nationwide Class)

185. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein. This Count is pled in the alternative to the Breach of Contract Count above.

186. Upon information and belief, Defendants funds their data-security measures entirely from their general revenue, including payments made by or on behalf of Representative Plaintiff and Class Members.

187. As such, a portion of the payments made by or on behalf of Representative Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of each payment allocated to data security is known to Defendant.

188. Representative Plaintiff and Class Members conferred a monetary benefit to Defendant. Specifically, they purchased goods and services from Defendants and/or their agents and provided Defendants with their PHI/PII. In exchange, Representative Plaintiff and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have their PHI/PII protected with adequate data security.

189. Defendants knew that Representative Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the PHI/PII of Representative Plaintiff and Class Members for business purposes.

190. Defendants enriched itself by saving the costs it reasonably should have expended in data-security measures to secure Representative Plaintiff's and Class Members' PHI/PII. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profits at the expense of Representative Plaintiff and Class Members by utilizing cheaper, ineffective security measures. On the other hand, Representative Plaintiff and Class Members suffered as a direct and proximate result of Defendants' decision to prioritize their profits over the requisite security.

191. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Representative Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures mandated by industry standards.

192. Defendants failed to secure Representative Plaintiff's and Class Members' PHI/PII and, therefore, did not provide full compensation for the benefit of Representative Plaintiff and Class Members.

193. Defendants acquired the PHI/PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

194. If Representative Plaintiff and Class Members knew that Defendants had not reasonably secured their PHI/PII, they would not have agreed to provide their PHI/PII to Defendant.

195. Representative Plaintiff and Class Members have no remedy at law.

196. As a direct and proximate result of Defendants' conduct, Representative Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of opportunity to determine how their PHI/PII is used, (iii) the compromise, publication, and/or theft of their PHI/PII, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, (vi) the continued risk to their PHI/PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect PHI/PII in their continued possession, and (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiff and Class Members.

197. As a direct and proximate result of Defendants' conduct, Representative Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

198. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Representative Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Representative Plaintiff and Class Members overpaid for Defendants' services.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on behalf of themselves and each member of the proposed National Class respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendants as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Representative Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from similar unlawful activities;

4. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiff's and Class Members' PHI/PII, and from refusing to issue prompt, complete, and accurate disclosures to Representative Plaintiff and Class Members;

5. For injunctive relief requested by Representative Plaintiffs, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiff and Class Members, including but not limited to an Order:

   a. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

   b. requiring Defendants to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards and federal, state or local laws;

   c. requiring Defendants to delete and purge Representative Plaintiff's and Class Members' PHI/PII unless Defendants can provide to the Court reasonable justification for the retention and use of such information when

weighed against the privacy interests of Representative Plaintiff and Class Members;

d. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiff's and Class Members' PHI/PII;

e. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

f. prohibiting Defendants from maintaining Representative Plaintiff's and Class Members' PHI/PII on a cloud-based database;

g. requiring Defendants to segment data by creating firewalls and access controls so that, if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

h. requiring Defendants to conduct regular database scanning and securing checks;

i. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Representative Plaintiff and Class Members;

j. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs and systems for protecting personal identifying information;

k. requiring Defendants to implement, maintain, review and revise as necessary a threat management program to monitor Defendants' networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested and updated;

l. requiring Defendants to meaningfully educate all Class Members about the threats they face as a result of the loss of their confidential PHI/PII to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law;

8. For all other Orders, findings and determinations identified and sought in this Complaint.

//

JURY DEMAND

Representative Plaintiffs, individually and on behalf of the Plaintiff Class(es) and/or Subclass(es), hereby demand a trial by jury for all issues triable by jury.

Dated: September 22, 2023

By:_____

Jared R. Cooper, Esq. (JC2975)
ROBINSON YABLON COOPER & BONFANTE, LLP
232 Madison Avenue, Suite 909
New York, New York 10016
Telephone: (212) 725-8566
Facsimile: (212) 725-8567
Email: jared@rycbinjury.com

Daniel Srourian, Esq.*
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
Telephone: (213) 474-3800
Facsimile: (213) 471-4160
Email: daniel@slfla.com

Counsel for Representative Plaintiff and the Proposed Class(es)

**Pro Hac Vice Forthcoming*

INTERNATIONAL BUSINESS MACHINES CORPORATION
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

40068272003988599
000 0000279 00000000 0001 0002 00140 INS: 0 0

[redacted]

27
10140

September 15, 2023

Notice of Data Breach

Dear Elaine D Malinowski:

This notice concerns an incident involving unauthorized access to personal information contained within a database used on the Janssen CarePath platform, a patient support platform that offers savings options and other patient support resources.

International Business Machines Corporation ("IBM" or "we") is a service provider to Johnson & Johnson Health Care Systems, Inc. ("Janssen"). IBM manages the application and the third-party database that supports Janssen CarePath. We are writing to inform you of a recent incident that may have involved unauthorized access to your personal information stored in Janssen CarePath. While we have no reason to believe that your information has been misused, we want to let you know what happened and the steps we have taken in response. This letter explains what happened, our response, and steps you can take to protect your information.

What happened: Janssen recently became aware of a technical method by which unauthorized access to the database could be obtained. Janssen then immediately notified IBM, and, working with the third-party database provider, IBM promptly remediated the issue. IBM also undertook an investigation to assess whether there had been unauthorized access to the database. While IBM's investigation identified, on August 2, 2023, that there was unauthorized access to personal information in the database, the investigation was unable to determine the scope of that access. As a result, we are notifying you out of an abundance of caution.

What information was involved: The personal information involved in this incident may have included your name and one or more of the following: contact information, and information about medications and associated conditions that were provided to the Janssen CarePath application. Your Social Security number and financial account information were not contained in the database or affected.

What we are doing: After being informed of the issue by Janssen, IBM and the third-party database provider promptly identified and implemented steps that disabled the technical method at issue. IBM also worked with the third-party database provider to augment security controls to reduce the chance of a similar event occurring in the future.

What you can do: We encourage you to remain vigilant by regularly reviewing your account statements and explanations of benefits from your health insurer or care providers with respect to any unauthorized activity. If you identify services that you did not receive or other suspicious activity, promptly report that activity to the institution that provided the report. Additional information on steps that you can take to protect against potential misuse of personal information can be found in the enclosed "Additional Resources" document, which we encourage you to review.